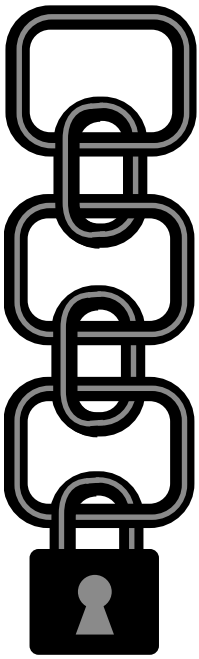
PROGRAM LOGICS FOR CERTIFIED COMPILERS

Separation logic is the twenty-first-century variant of Hoare logic that permits verification of pointer-manipulating programs. This book covers practical and theoretical aspects of separation logic at a level accessible to beginning graduate students interested in software verification. On the practical side it offers an introduction to verification in Hoare and separation logics, simple case studies for toy languages, and the Verifiable C program logic for the C programming language. On the theoretical side it presents separation algebras as models of separation logics; step-indexed models of higher-order logical features for higher-order programs; indirection theory for constructing step-indexed separation algebras; tree-shares as models for shared ownership; and the semantic construction (and soundness proof) of Verifiable C. In addition, the book covers several aspects of the CompCert verified C compiler, and its connection to foundationally verified software analysis tools. All constructions and proofs are made rigorous and accessible in the Coq developments of the open-source Verified Software Toolchain.

Andrew W. Appel is the Eugene Higgins Professor and Chairman of the Department of Computer Science at Princeton University, where he has been on the faculty since 1986. His research is in software verification, computer security, programming languages and compilers, automated theorem proving, and technology policy. He is known for his work on Standard ML of New Jersey and on Foundational Proof-Carrying Code. He is a Fellow of the Association for Computing Machinery, recipient of the ACM SIGPLAN Distinguished Service Award, and has served as Editor-in-Chief of *ACM Transactions on Programming Languages and Systems*. His previous books include *Compiling with Continuations* (1992), the *Modern Compiler Implementation* series (1998 and 2002), and *Alan Turing's Systems of Logic* (2012).



PROGRAM LOGICS FOR CERTIFIED COMPILERS

ANDREW W. APPEL
Princeton University, Princeton, New Jersey

ROBERT DOCKINS
Portland State University, Portland, Oregon

AQUINAS HOBOR
National University of Singapore and Yale/NUS College, Singapore

LENNART BERINGER
Princeton University, Princeton, New Jersey

JOSIAH DODDS
Princeton University, Princeton, New Jersey

GORDON STEWART
Princeton University, Princeton, New Jersey

SANDRINE BLAZY
Université de Rennes 1

XAVIER LEROY
INRIA Paris-Rocquencourt

CAMBRIDGE
UNIVERSITY PRESS
32 Avenue of the Americas, New York, NY 10013-2473, USA

Cambridge University Press is part of the University of Cambridge

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107048010

First published 2014

Printed in the United States of America

A catalog record for this publication is available from the British Library.

ISBN 978-1-107-04801-0 Hardback

This book is typeset in the Bitstream Charter font.
Font Copyright ©1989–1992, Bitstream Inc., Cambridge, MA.

in memory of

Kenneth I. Appel
1932–2013

a pioneer in computer proof

Contents

Road map

Readers interested in **the theory of separation logic** (with some example applications) should read Chapters 1–21. Readers interested in **the use of separation logic to verify C programs** should read Chapters 1–6 and 8–30. Those interested in **the theory of step-indexing** and **indirection theory** should read Chapters 35–39. Those interested in building models of **program logics** proved sound **for certified compilers** should read Chapters 40–47, though it would be helpful to read Chapters 1–39 as a warm-up.

Acknowledgments

I thank Jean-Jacques Lévy for hosting my visit to INRIA Rocquencourt 2005–06, during which time I started thinking about the research described in this book. I enjoyed research collaborations during that time with Francesco Zappa Nardelli, Sandrine Blazy, Paul-André Melliès, and Jérôme Vouillon.

I thank the scientific team that built and maintains the Coq proof assistant, and I thank INRIA and the research funding establishment of France for supporting the development of Coq over more than two decades.

Mario Alvarez and Margo Flynn provided useful feedback on the usability of VST 0.9.

Research funding for some of the scientific results described in this book was provided by the Air Force Office of Scientific Research (agreement FA9550-09-1-0138), the National Science Foundation (grant CNS-0910448), and the Defense Advanced Research Projects Agency (agreement FA8750-12-2-0293). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of AFOSR, NSF, DARPA, or the U.S. government.